NFV: Near Field Vibration Based Group Device Pairing

Zhiping Jiang(✉), Jinsong Han, Wei Xi, and Jizhong Zhao

Xi'an Jiaotong University, Xi'an, China
jiangzp.cs@gmail.com

Abstract. In this paper, we propose a group device pairing system called NFV to enable group communication using mobile device equipped with motion sensors. A group of people put their mobile devices on the table and wait for a secure connection. We propose a vibration-propagation based key delivery scheme to transmit a secure connection key among a group of trusted mobile devices. Based on this key, group users establish a confidential communication channel between their devices. NFV achieves group devices pairing without the complex operations needed in prior works. We implemented NFV using off-the-shelf Android smartphones. The experimental results shows the efficiency and security of our system.

Keywords: Vibration channel · Accelerometer · Pulse-width modulation · Ad hoc group pairing

1 Introduction

Mobile device has infiltrated into our daily lives, and it has enabled multiple new applications, such as photo sharing, mobile collaborative gaming [1], or mobile clouding [2,3], which require neighboring devices engaging in spontaneous interaction without prior configuration [4,5]. Numerous application scenarios based on *Human-to-Human* interaction could be observed or foreseen in the near future. For instance, conference attendees exchange notes and contact informations, or family members share files and photos.

Such promising desire requires neighboring devices to be aware of the intent and established a trustful connection. For example, most of existing solutions requires a prior wireless communication channel, such as WiFi or Bluetooth, to communication with target device, and the procedure is troublesome for most of the circumstances (scanning for neighboring devices and select particular target from a list [4]). Some other techniques even transmit a priori [6] or do synchronization action [7] in advance to make potential target devices aware of the purpose. Due to the energy constraint, mobile devices cannot provide continuous channel monitoring in the background to discover nearby devices, so that manual initiation is necessary for both transmission device and target devices.

S. Guo et al. (Eds.): CollaborateCom 2015, LNICST 163, pp. 129–140, 2016.
DOI: 10.1007/978-3-319-28910-6_12

Point & Connect (P&C) [5] initiates a connection with target device through a simple pointing gesture. Spartacus [4] has introduced a spatially-aware neighboring device interaction technique without configuration beforehand. By using a continuous audio-based low power listening, this system utilizes acoustic technique based on Doppler effect to enable devices to establish connection with particular target accurately. These two systems only achieve *One-to-One* device pairing, which is inconvenient to deploy in multiple devices' scenario for continuous connecting because it's time consuming.

In this paper, we seek to further abandon such inconvenience by accomplishing an ambient-aware context-based device *Group Pairing* strategy. We propose NFV, a mobile group file sharing and exchanging protocol, which enables users to interact with a nearby group of target devices without prior configuration. The proposed solution of NFV works as follows. A group of people put their mobile devices on the table for certain sharing purpose, and wait for a ad hoc connection. We assume all the devices on the table are legitimate users. We propose a vibration-propagation based key delivery scheme to establish a secure connection among a group of trusted mobile devices. An initiator on the table starts the connection by self-vibration, which could be broadcasted through the surface of the table as a secure channel and sensed silently by the surrounding devices on the same table. The self-vibration is programmable, so that the target devices capture the vibration through motion sensors, and extract information for generating connection key. Meanwhile, the initiator broadcasts encrypted information through high frequency acoustic signal, and receivers will decrypt the information through the information propagated through vibration. Although eavesdroppers could also record the encrypted information through public channel, they still cannot decrypt the original information. When original information is retrieved as shared key, all the target devices on the table will establish a secure connection through Wi-Fi Direct.

The main purpose of such design contains three folds. First of all, the key generation is convenient and secure, and the key distribution is much faster than traditional naive solutions, such as input key individually. Second, the protocol could defend Men-In-The-Middle attack. Even if the attacker could capture the encrypted information broadcast in the public channel, it still cannot retrieve the shared key for the connection. Then, we use zero-cost Wi-Fi Direct to replace the need for routers for connection, and it also consumes less power compared to Bluetooth.

The fundamental challenge here is how to capture such intention of patterned vibration on the table, and extract common information for generating shared key. That is, when placing on the surface of table, different material or structure of table may weaken the vibration intensity. Meanwhile, such intensity would be influenced by the distance between the target device and the tapping location, or even overwhelmed by the internal noise of motion sensor if the vibration is mild. It is a non-trivial problem to detect the sharing intention among devices robustly. Another equal challenge comes from the common key delivery strategy to establish secure communication channel.

Compared with other existing works, the main contribution of this paper is as follows:

1. We propose a novel and secure ambient-aware devices group pairing protocol initiated by simple self-vibration.
2. We develop a pulse-width modulation (PWM) based key delivery scheme based on the tiny vibration broadcast through the surface of the table, and establish a secure group communication channel without prior connection.
3. We implement NFV on Android smartphones and tablets, and evaluate the system using various device models under different interaction scenarios. And the evaluation indicates that the protocol is reliable and secure.

2 System Overview

NFV offers a group device sharing solution in close proximity, and works with state-of-the-art mobile devices with standard hardware settings. It does not rely on any additional devices or OS modification to establish a group device pairing.

2.1 Application Scenarios

The main purpose of this application is to simplify information sharing, file synchronising, and message exchanging. The typical setting for a NFV application scenario is that a group of mobile devices (*e.g.*, smartphones, tablets) are located within a short range, and intent to establish a connection. The Fig. 1 illustrates showcase of scenario in a conference room, where users intends to pair their devices on the table to synchronize their meeting notes. The system do not require extra equipments for establishing both public and secure channels to exchange information, and both the initiator and the target devices extract secret key from the exchange channel to establish a connection.

Fig. 1. Motivation scenario

NFV operates when the participated devices are stationarily located on the same surface, such as table. It makes use of the desk as a broadcast medium, and transmit secret information through the surface. NFV targets a group pair of devices that initiate interaction at with short delay, and all the devices on the same surface extract the same key to establish instantaneous connection automatically, such as WiFi direct.

2.2 Design Guidelines

NFV explore an ambient-aware pairing initiation design without taking any assisted actions. A group of users will prepare the interaction by putting their devices on the desk. An initiator will broadcast secret information through vibration according to certain pattern, and transmit coded information through acoustic signal. The software and the motion sensors in modern smart mobile devices will work together to overcome the limitation of devices.

Although we assume the devices on the same desk are all trustful, we still provide a verification function to validate the target devices in case of eavesdroppers nearby. For example, attackers can easily capture the acoustic signal or hear slight vibration noise through microphone. The main purpose of the verification function is guarantee the pure audio information cannot retrieve the secret key for connection.

NFV also has to seek the robustness of the system when initiating interaction, and the design complexity. The design of NFV should be robust under a variety of imperfect opening environment, especially when it comes to the desk with different materials and thickness, or covered with tablecloth. It should also functions well facing unpredicted environment noises.

2.3 Design Challenges

Our protocol typically contains three stages, connection attempt detection, secure common key delivery, and group communication channel establishment.

- Due to the internal mechanism of motion sensors, the measurement noise and ambient-variance may influence the sensory data, which may hinder the device to detect the pairing attempt at the first place. Especially the devices are placed on the table freely and randomly, and sometimes the distance between the devices and the knocking location is large.
- In order to establish a secure group communication channel, a shared secure key is needed. However, improper prior communication for key exchange in public channel is insecure, generate shared key through the vibration broadcast from simply knocking is difficult.
- Despite the variance of sensory data, the pattern of general vibration, especially the Simple harmonic vibration is similar. If the key delivery strategy is designed based on such coarse-grained pattern, attackers are more likely to launch collision attack, and eventually break the secure communication. Therefore, the shared key should not depend on coarse-grained knocking vibration.

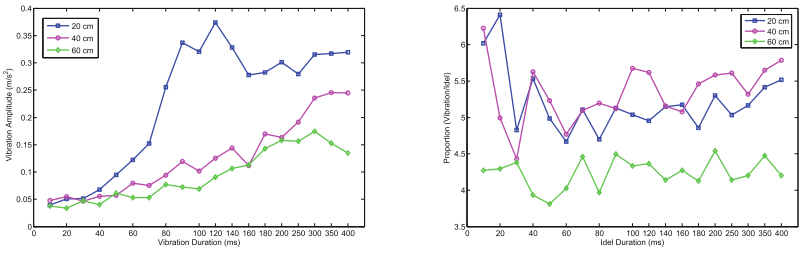
3 System Design

NFV delivery the secret session password via two distinct channel, the secret vibration channel, and an arbitrary public channel. Given a session password pw_s to be shared with legitimate users, we delivery the encrypted version of pw_s, *i.e.* $enc(pw_s, k)$ via public channel, and the short key k via vibration channel. Upon receiving these two pieces of information, the receiver decrypts $enc(pw_s, k)$ with k, and use pw_s to establish the ad-hoc network.

3.1 Vibration Channel Analysis

Since NFV requires all the devices in the group communicate through both acoustic channel and vibration channel. Therefore, in this section, we will mainly discuss our preliminary analysis on both vibration channel detection and propose the system architecture based on our analysis.

Current mobile devices customize vibrator to provide a vibration intensity, frequency or duration in certain pattern to deliver tactile notification to users [8]. However, the vibration provided by the phones are subtle and private [9], and it only have binary settings (on or off), which limits the communication capability. Haptics researches suggest using vibrotactile patterns to deliver ambient information on mobile phones [10]. Motivated by such works, we explore the capacity of vibration communication on both transmission and receiving. Ideally, there would be a specific vibration pattern broadcasted from the initiator, and all the receivers on the same desk receive the vibrotactile message through motion sensors (*e.g.* accelerometer and gyroscope). However, generating various distinguishable vibrotactile could be difficult on commodity mobile devices, although the API for Android support user-defined durations for which to turn on or off the vibrator in milliseconds. Therefore, one technique issue has to be conquered is how to retrieve the initial cue from the sensory data (Fig. 2).



(a) Detected Vibration Amplitude (b) Vibration to Idle

Fig. 2. Vibration analysis.

PeopleTones [11] adjusts the duty cycle of the vibrotactile actuator to generate vibration in various levels. However the amplitude of the vibration cannot be

detected precisely because of the various distance between the initiator and the receiver. The vibration generates mechanical wave, which spreads on the surface of the desk, and the target device on the same surface could record the vibration through motion sensors. Empirically, the amplitude of the sensed vibration is affected by three main factors: the distance between the vibrator and the receiver, the material of the surface where the devices are put, and the vibration frequency and duration. We conducts a comprehensive experiments on detecting the vibration broadcast from the initiator device.

The Android provides API to operate the vibrator on the devices, and the vibration pattern is determined by the input array of ints that are the duration for which to turn on and off the vibrator in milliseconds. Generally, due to the internal noise of motion sensor, the first issue is distinguishing the vibration from continuous sensory data. In this experiment, we deploy two Nexus 5 smartphones on the table with 20 cm to 60 cm apart. We take two set of experiments to handle how long should the vibrator work to be detected, and how long should the vibrator to rest to distinguish two continuous vibration. We set one phone to vibrate from 10 ms to 400 ms with 500 ms idle between two successive vibrations, and plot the result in Fig. 3(b). In this figure, we learn two facts: with the vibration duration increases, the sensed vibration from accelerometer increase as well; and shorter distance between sender and receiver, the more sensitive the receivers' motion sensor.

Figure 3(a) illustrates the proportion of vibration to idle in acceleration under the circumstance that the sender vibrator 500 ms and rest from 10 ms to 400 ms until next vibration. It is obvious that when the idle time period is only 10 ms, the proportion is relatively high, especially when the distance between the two devices is close. During this experiment, the receiver cannot distinguish each vibration clearly, the receiver only consider this as a continuous vibration. When the interval increases, the device could distinguish the two successive vibration from the sensory data, because of the obvious vibration amplitude difference. We thought the accelerometer only capture measurement noise when idle, which turned to be wrong eventually. The device vibrating on the table generates mechanical wave, which broadcasts through the table surface. And such vibration transferred into simple harmonic vibration for each particle on the face of the table. According to Hooke's Law, the particle on the table will continuous vibrating even if the source stops vibrating. In this case, the accelerometer captures both simple harmonic vibration and measurement noise during idle period, and longer idle period indicates more noise. Therefore, the proportion increase when the idle duration grows.

3.2 PWM-Based Vibration Channel

In this part, we have to design the encoding pattern to fulfill two goals: increasing the transmission bit rate, and guaranteeing the correctness of decoding from vibration. In the previous section, we notice that both the duration of vibration and idle should last longer than 80 ms to be identified by the target devices. Pursuing a balanced protocol, we propose an pulse-width modulation (PWM) based

vibration channel. Pulse-width modulation uses a rectangular pulse wave whose pulse width is modulated resulting in the variation of the length of the vibration. To balance the transmission rate and the error rate, the pulse idle is set as 80 ms to achieve a distinguishable gap between pulses. Each pulse has 4 candidate length representing a 2-bit code. The pulse lengths are 80/100/120/140 ms. In this way the average transmission rate is about 10 bit/s, *i.e.* it only takes 4 s to transmit the key. That is acceptable in practical scenarios.

3.3 Demodulation

NFV communicate via the vibration propagation through the table medium. Ideally, when the transmitter stops vibration, the medium should stop soon. However, in real table medium, the vibration still remains long after the transmitter stops. It brings big challenge to the receiver side. The oscillation of table medium will introduce inter-symbol interference and vague timming at the received signal, which makes it hard to distinguish the "0" and "1" of modulated PWM signal. To help precisely determine the timing at the receiver side, the transmitter plays short beeps every 20 ms, which is synchronized with the timing of vibration channel PWM. These short beeps allow the receivers to synchronize the demodulator with PWM signal and eventually decode the secret key.

3.4 Acoustic Channel and Group Pairing

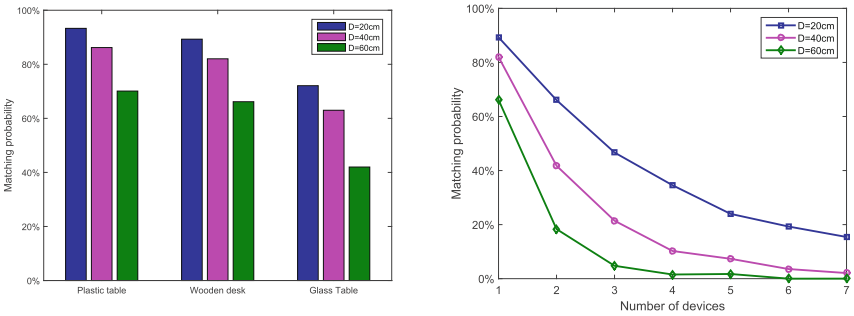
NFV demands another communication channel to broadcast the encrypted session key and necessary protocol signals. This channel could be an insecure or secure channel. Pursuing the robustness and efficiency, we choose acoustic channel. Each device randomly chooses a 200 Hz bandwidth between 17 kHz to 19 kHz and then claims its possession to the channel with a random delay. If channel collision is detect, the latter one will try another channel. We adopt the simple 4-FSK modulation due to its robustness and asynchronous property. According to our real world, over 150 bit/s transmission rate can be achieved, which is acceptable in our prototype.

Once the session key is successfully decrypted. All devices will initiate Wi-Fi Direct connections with the identical session key. In this way, a group pairing is established.

4 Prototyping and Evaluation

4.1 Prototype Implementation

We implement NFV on Android platform. Our test devices include 2×Nexus 4, 3×Nexus 5, and 2× Samsung Galaxy S4. The accelerometer sampling rate is 100 Hz for all devices.



(a) Transmission Success Rate on Different Material

(b) Devices Pairing Success Rate

Fig. 3. (a) Transmission success rate on different material. (b) Group pairing success rate in different distance.

4.2 Prototype Performance Evaluation

Performance of Vibration Channel. We first evaluate the transmission success rate of 32-bit key over vibration channel. We conduct 20 times transmission on different table material and the distance varies from 20 cm to 60 cm. The test table material are plastic table, wooden desk, and glass table. They are usually seen in practical scenario.

Figure 3(a) shows the result. We see that the success rate drops along with the table material. The stronger the table material, the lower success rate. This is because, the stronger material is related to higher density, which requires higher energy to vibrate the table. The success rate also drops with the mutual distance. This is because the longer the distance, the smaller the vibration energy is at the receiver. Based on the test, we recommend the suitable distance between devices is within 40 cm.

Capacity of NFV. Due to the transmission error found in the vibration channel, the success rate of establishing a NFV channel decreases along with the number of devices. We conduct experiments to evaluate its performance.

Figure 3(b) shows the result. We see clearly from the figure that, as the distance among devices grows the success rate drops rapidly. When within 20 cm, the average success rate is more than 70 % for 5 devices. The success rate drops even faster when the distance goes to 60 cm. In this case, it can only support 2 devices pairing.

4.3 Security Evaluation

Acoustic Leakage. The security of NFV is based on an assumption that, the eavesdroppers seated at another desk cannot recover the key extracted from local desk vibration. We use mutual information to evaluate the similarity of acoustic

signal and vibration signal. The acoustic signal is low-passed to 0–100 Hz, and we then use the same protocol to extract the initial key from the acoustic signal.

Table 1 shows the correlation between vibration signal and the acoustic under different environmental noise level. The result shows that when in quiet environment the vibrator's noise can be captured with some success rate regardless of table material. While in relatively noisy and very noisy environment, the correlation drops rapidly, indicating that the attacker's very low probability to guess the key.

Table 1. Acoustic leakage evaluation

	-80 db	-60 db	-40 db
Plastic table	0.43	0.321	0.11
Wooden desk	0.37	0.22	0.05
Glass table	0.49	0.32	0.08

5 Related Work

NFV leverages built-in vibrator and motion sensors on commodity mobile devices for both initiating connection and intention detection. It also utilizes microphones and speakers on the devices to transmit and listen interaction information. In this section, we review previous works about device interacting and acoustic sensing.

5.1 Device Pairing and Interaction

Interacting with nearby devices usually requires candidate devices to be identified by name so as to be retrieved during the scanning process. When connecting, users have to choose the target manually which heshe thinks is right. SyncTap [12] requires both users to press and release the button on the devices simultaneously to achieve pairing. Amigo [13] uses shared radio environment to prove their location proximity for pairing devices, but still use traditional synchronous action to accomplish pairing.

Interacting with neighboring mobile devices requires each devices being capable of both selecting the right target and interacting. [14] indicates that touching, scanning, and pointing are the most basic three stages for mobile device interacting with smart objective. Point & Connect (P&C) [5] utilizes time difference of arrivals of acoustic signals to initiate interactions in close proximity by pointing phone towards the intended target. However, this system requires users to open the broadcast channel manually so as to allow others to discover, which is troublesome. Spartacus [4] is quite similar to [5], which utilizes Doppler effect to initiate a connection with neighboring devices. The largest difference is that it runs as a system service to detect potential interaction intentions periodically

and uses duty-cycled audio listening mechanism to save energy consumption. SoundWave [15] also uses Doppler effect to detect user gestures for human-computer interaction in close range. The detection of frequency shift achieved with high accuracy in this system since the computer plays both the transmitter and the receiver to double the frequency shift. Shake Well Before Use [16] capture sensory data from synchronous action, which could be used to detect the right pairing devices.

Existing works of detecting neighboring devices and interaction requests usually require additional equipments. PANDAA [17] relies on ambient sound to achieve centimeter-level device locating accuracy in indoor environment without using extra infrastructures, and none human-intrusive. Polaris [18] provides an orientation-dependent indoor device interaction techniques without additional devices.

5.2 Acoustic Sensing

Acoustic sensing on mobile devices has been used in several purposes. SurroundSense [19] utilizes audio data with sensory information to infer logical location. CenceMe [20] analyzes human social activities based on human conversations. SoundSense [21] employs signal processing pipeline for audio sensing, and distinguish music from noise. Similarity, Auditeur [22] detects acoustic events in real-time based on mobile-cloud platform [2,3,23]. There are some other applications which handles different types of sounds. For example, Nericell [24] detects horn of vehicles, iSleep [25] monitors people's sleep state using acoustic sensing, Ear-phone [26] is used to monitor noise pollution in urban environment. SwordFight [1] continuously outputs accurate distance between two smartphones using time different of acoustic signal's arrival.

6 Conclusion

This paper introduce a secure and efficient group device association method based on shared table vibration. We introduce a two-step process to establish such a secure ad hoc association. The robust Golay coding is first adopted to extract a session initialization vector from the raw accelerometer readings. This session initialization vector is passed to an secure group key exchange process to generate a high entropy session key. We prototype our system on off-the-shelf smartphone. Extensive evaluations have proved the security, efficiency, and convenience of our system.

References

1. Zhang, Z., Chu, D., Chen, X., Moscibroda, T.: Swordfight: enabling a new class of phone-to-phone action games on commodity phones. In: ACM MobiSys 2012 (2012)

2. Liu, F., Shu, P., Jin, H., Ding, L., Yu, J., Niu, D., Li, B.: Gearing resource-poor mobile devices with powerful clouds: architectures, challenges, and applications. IEEE Wirel. Commun. **20**(3), 14–22 (2013)
3. Liu, F., Shu, P., Lui, J.: Appatp: an energy conserving adaptive mobile-cloud transmission protocol (2015)
4. Sun, Z., Purohit, A., Bose, R., Zhang, P.: ACM MobiSys 2013 (2013)
5. Peng, C., Shen, G., Zhang, Y., Lu, S.: Point & connect: intention-based device pairing for mobile phone users. In: ACM MobiSys 2009 (2009)
6. Goodrich, M.T., Sirivianos, M., Solis, J., Tsudik, G., Uzun, E.: Loud and clear: human-verifiable authentication based on audio. In: IEEE ICDCS 2006 (2006)
7. Hinckley, K.: Synchronous gestures for multiple persons and computers. In: ACM UIST 2003 (2003)
8. Barton, S.: Programmable notifications for a mobile device. US Patent App. 11/116,860, 28 April 2005
9. Hansson, R., Ljungstrand, P., Redström, J.: Subtle and public notification cues for mobile devices. In: Abowd, G.D., Brumitt, B., Shafer, S. (eds.) Ubicomp 2001. LNCS, vol. 2201, pp. 240–246. Springer, Heidelberg (2001)
10. Poupyrev, I., Maruyama, S., Rekimoto, J.: Ambient touch: designing tactile interfaces for handheld devices. In: ACM UIST 2002 (2002)
11. Li, K.A., Sohn, T.Y., Huang, S., Griswold, W.G.: Peopletones: a system for the detection and notification of buddy proximity on mobile phones. In: ACM MobiSys 2008 (2008)
12. Rekimoto, J., Ayatsuka, Y., Kohno, M.: SyncTap: an interaction technique for mobile networking. In: Chittaro, L. (ed.) Mobile HCI 2003. LNCS, vol. 2795, pp. 104–115. Springer, Heidelberg (2003)
13. Varshavsky, A., Scannell, A., LaMarca, A., de Lara, E.: Amigo: proximity-based authentication of mobile devices. In: Krumm, J., Abowd, G.D., Seneviratne, A., Strang, T. (eds.) UbiComp 2007. LNCS, vol. 4717, pp. 253–270. Springer, Heidelberg (2007)
14. Rukzio, E., Leichtenstern, K., Callaghan, V., Holleis, P., Schmidt, A., Chin, J.: An experimental comparison of physical mobile interaction techniques: touching, pointing and scanning. In: Dourish, P., Friday, A. (eds.) UbiComp 2006. LNCS, vol. 4206, pp. 87–104. Springer, Heidelberg (2006)
15. Gupta, S., Morris, D., Patel, S., Tan, D.: Soundwave: using the doppler effect to sense gestures. In: ACM CHI 2012 (2012)
16. Mayrhofer, R., Gellersen, H.-W.: Shake well before use: authentication based on accelerometer data. In: LaMarca, A., Langheinrich, M., Truong, K.N. (eds.) Pervasive 2007. LNCS, vol. 4480, pp. 144–161. Springer, Heidelberg (2007)
17. Sun, Z., Purohit, A., Chen, K., Pan, S., et al.: Pandaa: physical arrangement detection of networked devices through ambient-sound awareness. In: ACM Ubicomp 2011 (2011)
18. Sun, Z., Purohit, A., Pan, S., Mokaya, F., et al.: Polaris: getting accurate indoor orientations for mobile devices using ubiquitous visual patterns on ceilings. In: ACM MCSA 2012 (2012)
19. Azizyan, M., Constandache, I., Roy Choudhury, R.: Surroundsense: mobile phone localization via ambience fingerprinting. In: ACM MobiCom 2009 (2009)
20. Miluzzo, E., Lane, N.D., Fodor, K., et al.: Sensing meets mobile social networks: the design, implementation and evaluation of the cenceme application. In: ACM SenSys 2008 (2008)

21. Lu, H., Pan, W., Lane, N.D., Choudhury, T., Campbell, A.T.: Soundsense: scalable sound sensing for people-centric applications on mobile phones. In: ACM MobiSys 2009 (2009)
22. Nirjon, S., Dickerson, R.F., Asare, P., Li, Q., Hong, D., et al.: Auditeur: a mobile-cloud service platform for acoustic event detection on smartphones. In: ACM MobiSys 2013 (2013)
23. Shu, P., Liu, F., Jin, H., Chen, M., Wen, F., Qu, Y.: etime: energy-efficient transmission between cloud and mobile devices. In: Proceedings IEEE on INFOCOM 2013, pp. 195–199. IEEE (2013)
24. Mohan, P., Padmanabhan, V.N., Ramjee, R.: Nericell: rich monitoring of road and traffic conditions using mobile smartphones. In: ACM SenSys 2008 (2008)
25. Hao, T., Xing, G., Zhou, G.: iSleep: unobtrusive sleep quality monitoring using smartphones. In: ACM SenSys 2008 (2008)
26. Rana, R.K., Chou, C.T., Kanhere, S.S., Bulusu, N., Hu, W.: Ear-phone: an end-to-end participatory urban noise mapping system. In: ACM IPSN 2010 (2010)